

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

11/15/2013

SUBJECT:

Multiple Vulnerabilities in Google Chrome Could Allow Remote Code Execution.

OVERVIEW:

Multiple vulnerabilities have been discovered in Google Chrome that could allow remote code execution or cause denial-of-service conditions. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Google Chrome Prior to 31.0.1650.57

Google Chrome on Android Devices Prior to 31.0.1650.59

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**

Small business entities: **High**

Home users: High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Google Chrome. These vulnerabilities were demonstrated at the recent PwntoOwn contest. Details of the vulnerabilities are as follows:

- An integer overflow vulnerability that could lead to remote code execution.
- A vulnerability that could allow an escape from the Google Chrome application sandbox, which separates the browser's processes from the operating system.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable Google Chrome products immediately after appropriate testing by following the steps outlined by Google.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or un-trusted sources.

REFERENCES:

Google:

http://googlechromereleases.blogspot.com/2013/11/stable-channel-update_14.html

HP:

<http://www.hppwn2own.com/chrome-nexus-4-samsung-galaxy-s4-falls/>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6632>

Security Focus:

<http://www.securityfocus.com/bid/63729>